A Risk Informed Approach to Reliability Requirements Tailoring

John Klohoker, Jet Propulsion Laboratory, California Institute of Technology

Key Words: reliability, risk, requirements, tailoring, RIDM

SUMMARY & CONCLUSIONS

Every institution has their "recipe" for success. Cell phones and personal computers seem like they are designed to be obsolete in 2-3 years. Automobiles seem like they are designed to have a power train failure within 1000 miles of the extended warranty expiration; at least that's been my experience. The Jet Propulsion Laboratory (JPL) is not any different. JPL has a tried and proven recipe for success because in space things can't fail. Or else.

However, in today's competitive environment and funding limitations, that recipe for success is being challenged and the resultant increased risk accepted.

This paper will describe JPL's Risk Informed Decision Making (RIDM) approach to tailoring reliability requirements based on mission classification and other project characteristics.

1 INTRODUCTION

At JPL, reliability is not designed to meet a specified quantitative value. Quantitative reliability techniques are primarily used for reliability trade studies and risk assessments. Reliability is designed into the hardware through the imposition of design principles and flight project practices. JPL Reliability Engineering verifies compliance with the design principles and flight project practices through the use of various system, circuit, and electro-mechanical analyses. These include electronic parts-stress; worst-case circuit; failure modes, effects, and criticality; single-event effects; sneak-circuit; and fault-tree analyses. Some analyses, such as FMECAs and fault trees, can be performed at various levels and/or on specific hardware types such as mechanisms.

Projects begin with a baseline (institutional) set of process and product requirements that represents the standard approach to reliability engineering for low-risk missions. Through a risk-informed decision-making (RIDM) process, the baseline requirements are tailored for a specific project based on project constraints, mission characteristics, and the design characteristics for specific hardware items. Departures from the baseline approach are assessed for potential implementation and mission risks and are communicated and documented appropriately.

Using the JPL RIDM approach to the tailoring of reliability requirements, JPL Reliability personnel engage with project personnel early in the development life cycle to develop project-specific requirements intelligently, trading risk for other project constraints (e.g., budget, schedule).

2 WHERE TO BEGIN

The risk-informed decision-making (RIDM) tailoring process begins during Phases A/B; project formulation. The tailoring begins well before the implementation Phases C/D and continues throughout the project life cycle. The first round of tailoring occurs when projects and line organizations negotiate project-specific requirements, schedules and other aspects of project implementation. The results of the initial tailoring is documented in requirements documents/plans, work agreements, and waivers (as-needed).

For reliability, subsequent tailoring is often necessary to address requirements changes, design evolution, hardware capability, budget and schedule constraints, test failures, and other project nuances. Depending on the nature of the tailoring, the changes are captured in waivers, interoffice memoranda, work agreement updates, and/or requirements document revisions via Engineering Change Requests (ECRs) When project characteristics change, it's important that all prior reliability tailoring is reviewed and the associated risk re-evaluated. For example, if system redundancy is changed, then the risk associated with waiving certain analyses could change.

In general, the RIDM tailoring process includes the following key steps:

1 *During formulation, work with project personnel to understand the project characteristics*

2 *Work with project personnel to identify tailoring opportunities and the associated risks*

3 *Develop project specific requirements and document them using the matrices in this paper as guidance*

4 *Review and get approval from line and project management*

5 *Document exceptions to baseline requirements and residual risks using waivers as-needed*

6 *Throughout the project development cycle, work*

with project personnel to understand new and changing project requirements, nuances , and constraints

7 *Work with project personnel to identify tailoring options to accommodate new developments*

8 *Review with line and project management*

9 *Document additional changes and residual risks using ECRs, waivers, IOMs, etc. as appropriate*

When working with one or more partnering institutions (e.g., NASA, foreign governments), each partner typically follows their own methodologies for reliability assurance, environmental assurance, and anomaly reporting and resolution. When working with system and subsystem subcontractors (which could include NASA and foreign companies), JPL typically negotiates contracts such that subcontractors are required to follow JPL methodologies. Depending on what is specified in the contract, deviations and exceptions are accepted and risk assessed through the waiver process.

3 PROJECT CHARACTERISTICS

The tailoring process begins with identifying and understanding project characteristics, including the mission/instrument risk classification (per NASA NPR 8705.4), project constraints, mission characteristics, and design characteristics. The project reliability engineer(s) are encouraged to work with project design personnel to gather the relevant project data.

When tailoring, the project constraints that are taken into consideration include:

- Mission Class: NASA risk classification
- Risk Posture: project visibility, perceived priority amongst other projects, national/international significance
- Project management responsibility, partnering institutions, and significant subcontractors
- Budget and funding profiles
- Schedule: development time, launch window
- Single point failure policy

In addition to the project constraints, the tailoring process also needs to take into consideration the Mission Characteristics. The mission characteristics include:

- Objectives/Requirements: Level 1 requirements, threshold mission requirements, mission success criteria
- Type of mission: Orbiter, Lander, Fly-By
- Destination(s)
- Lifetime
- Critical maneuvers/events: entry/descent/landing, orbit insertion, complex encounters, other unique risk elements
- Mission environments

The tailoring process also needs to consider the design characteristics, including:

- Complexity: mass/power/volume constraints, environmental sensitivities
- Hardware pedigree: new design, inherited, commercial
- Software complexity and inheritance
- Provider: JPL in-house, supplier
- In-flight operating time
- Redundancy, degraded modes of operation
- Power source(s)
- Usage: similar to previous applications, environment similar to or bounded by previous experience base
- Model availability and uncertainty

In addition to mission/instrument risk classifications from NASA, JPL assigns projects to Type I, II, or III. JPL Type I primarily includes Class A, B, and C flight projects; Type II primarily includes Class D flight projects and other flight projects that are not risk classified; Type III primarily includes non-spaceflight projects (e.g., sounding rockets, balloons, ground-based projects).

Each project is identified as belonging to one of five groups based on JPL type assignment, NASA risk classification, and other distinguishing qualities (see Table 1 below). Generally speaking, there is minimal tailoring of the baseline requirements for the Type 1 project groups in comparison to the Type II project groups.

4 RELIABILITY REQUIREMENTS TAILORING

Reliability assurance programs comprise the set of well-defined, closed-loop activities performed over the life of a flight project to verify that the circuits, boards, assemblies, subsystems, and system will meet their performance requirements under the stated conditions for the specified period. During the design phase, these activities include analyses to ensure proper designed-in reliability consistent with

	Type I			Type II	
	Class A Highest Cost Lowest Risk	**Class B High Cost Low Risk**	**Class C Medium Cost Medium Risk**	**Class D+ Low Cost Med/High Risk**	**Class D− Lowest Cost Highest Risk**
Priority	Very high	High	Medium to high	Low to medium	Lowest
Design Complexity	Very high (e.g., multiple instruments, redundant systems)	High	Low to medium (e.g., single instrument, heritage bus)	Low (e.g., some use of commercial parts)	Very low (e.g., extensive use of commercial parts)
Schedule	Critical launch window, critical maneuvers and/or events	Critical launch window	Noncritical launch window	Noncritical launch window, short development schedule	Noncritical launch window, shortest development schedule
Mission Lifetime	>5 years	2–5 years	2–3 years	<2 years	<1 year
Mission Environments	Harsh or unknown	Harsh or unknown	Benign or known	Benign or known	Benign or known
Single-Point Failures (SPFs)	Could result in total mission failure (i.e., not meeting minimum mission success criteria)	Could result in significant but not catastrophic loss (i.e., still meeting mission objectives)	Mission-critical SPFs acceptable; retrieval or on-orbit maintenance may be possible	Mission-critical SPFs acceptable; retrieval or on-orbit maintenance may be possible	Mission-critical SPFs acceptable; retrieval or on-orbit maintenance unlikely
Examples	Cassini, Mars 2020, Europa Clipper	Dawn, Juno, Kepler, MSL CheMin	SMAP, Aquarius, Phoenix, NISAR	CAL, DSAC, ECOSTRESS	CubeSats (e.g., ASTERIA, RainCube)

Table 1. JPL Project Types

mission requirements.

During the assembly phase, these activities are intended to provide objective evidence that functionality has been verified and validated adequately; faults, defects, and other latent issues have been found; and all issues are resolved or closed out to an acceptable level of risk. Project reliability engineers (PREs) provide technical oversight and review to ensure that reliability assurance activities are consistent with program requirements.

During the architectural phase, PREs work with project personnel to generate system reliability analyses; these analyses can help inform tailoring of requirements for lower-level design analyses. Through concurrent engineering with PRE involvement in system reliability analyses, design issues can be discovered early in the project development cycle, reducing the need for costly rework or high-risk waivers.

4.1 Baseline Reliability Requirements

The baseline reliability requirements are specified in the following documents.

- Flight Project Practices
- Design Principles
- Reliability Assurance Requirements Document
- Reliability Analyses Guidelines for Flight Hardware

PREs work with projects to tailor these baseline requirements based on project characteristics. This tailoring considers a variety of areas, including

- Methodology (e.g., scope, RSS vs. EVA, margins)
- Level of independent review
- Project reliability assurance plan
- Reliability analyses (generation, independent review)
- Documentation (waivers, local waiver process, DADs, IOMs, RATS)

Through tailoring, PREs develop a project-specific reliability assurance program that uses RIDM to allocate resources to address the identified risks.

4.2 Reliability Requirements Tailoring Overview

The reliability requirements tailoring process typically begins during formulation, when PREs meet with project personnel to understand project characteristics and to identify

risks associated with the project, system, hardware, and software. PREs then work with project personnel to assess the identified risks for severity of mission consequence and probability of occurrence and to rank/prioritize them accordingly. In collaboration with the project, PREs tailor the baseline requirements to best address the prioritized risks within project constraints. After documenting the tailored requirements into the project Safety and Mission Assurance Plan, PREs review the tailoring options and associated risks with project and line management.

Tailoring of reliability requirements continues throughout the project development cycle to accommodate requirements changes, design evolution, hardware capability, budget and schedule constraints, and other project nuances and constraints. This tailoring is typically captured in waivers, IOMs, design/analysis discrepancies (DADs), and the Reliability Analysis Tracking System (RATS) as appropriate.

The reliability requirements tailoring matrix was developed as a tool to assist in the tailoring process. The matrix includes

- Baseline reliability requirements
- Unique conditions, trades, and other tailoring considerations
- Mission and implementation risk associated with tailoring options
- Recommended approach for JPL Type I and II projects
- Lessons learned, examples, and other tailoring guidance

The reliability requirements tailoring matrix is intended to be used as a guide as opposed to a menu of what requirements to leave in and what to leave out.

5 CONCLUSION

The RIDM approach to tailoring brings project design and reliability personnel together to engage in discussions with regards to reliability requirements and potential risks, both project implementation and mission objective risks. RIDM has proven to be a valuable approach as both project and mission assurance personnel have reached mutual agreements with regards to reliability requirements tailoring and the associated risks as the project moves forward towards the implementation phase.

The research was carried out at the Jet Propulsion Laboratory, California Institute of Technology, under a contract with the National Aeronautics and Space Administration.

BIOGRAPHY

John Klohoker, Electronics Engineer
Jet Propulsion Laboratory, California Institute of Technology
Project Reliability Engineering (5131)
Pasadena, CA 91109

e-mail: john.j.klohoker@jpl.nasa.gov

John Klohoker is the Project Reliability Engineer for a Technology Development Project at the Jet Propulsion Laboratory (JPL) in Pasadena, CA. Prior to becoming the Project Reliability Engineer, John was the Group Supervisor for the Product and Circuit Reliability Group for 10 years. He obtained his BSEE from Purdue University and has over 38 years of experience in the Mission Assurance discipline.